



Advanced eDiscovery for Microsoft 365

Lab Guide

This document is provided "as-is". Information and views expressed in this document, including URL and other Internet Web site references, may change without notice. You bear the risk of using it.

This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal, reference purposes.

© 2019 Microsoft. All rights reserved.

Contents

Prerequisites.....	5
Demo home page and login.....	5
User Accounts.....	5
First-time Post-Install Steps.....	7
Advanced eDiscovery for Microsoft 365 Pre-demo Setup Steps.....	Error! Bookmark not defined.
Advanced eDiscovery for Microsoft 365 Demo Steps	12
Microsoft 365 Compliance Center: Case Creation.....	12
Create a new Case	12
Settings – Analytics settings and / or basic information	13
Custodian Management & Communications.....	13
Add Custodians to a Case.....	13
Create and send hold notification.....	15
View custodian audit activity.....	17
Searches.....	18
Create a search	18
Preview results and search stats.....	18
Add to a review set.....	19
Review set Management	21
Create a review set	Error! Bookmark not defined.
Configure tag panel	21
Understand differences between search results with load sets	23
Load non-Office 365 data.....	24
Review and Tagging	25

Run eDiscovery analytics.....	25
Query within a review set.....	26
Annotate a document.....	27
Tag a document.....	Error! Bookmark not defined.
Bulk tagging.....	28
Jobs.....	29
Overview of jobs.....	29
Errors.....	29
Error reporting.....	29
Export.....	30
Download query results.....	30
Export query results to Microsoft provided Azure Blob.....	30
Conclusion.....	31
No Click steps.....	31
Advanced eDiscovery for Microsoft 365 Reset Steps.....	Error! Bookmark not defined.
Portal Content.....	32
Advanced eDiscovery for Microsoft 365 Post-Install Steps.....	Error! Bookmark not defined.
Figure 1:.....	Error! Bookmark not defined.

Prerequisites

Demo home page and login

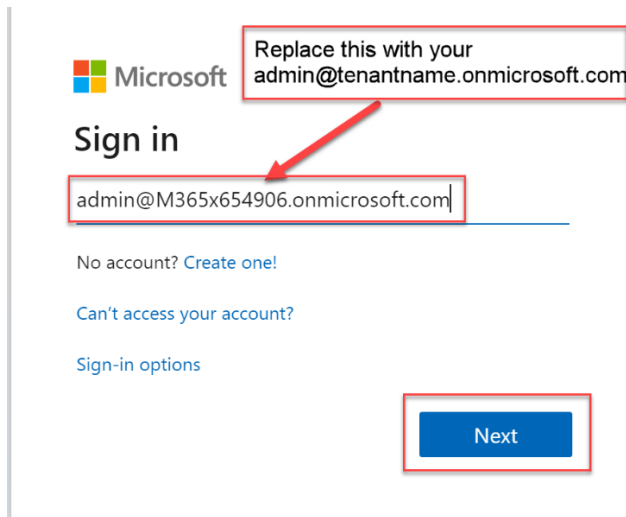
Before you start you should have completed the "Getting started with Microsoft 365 Compliance Master Class Labs". If you have not completed this you will not be able to do this lab. You can find this document which you can download from <https://aka.ms/m365masterclass-labs> Each tenant will take 24 hours to provision so its important that you complete this prior to Tuesday when the event starts.

User Accounts

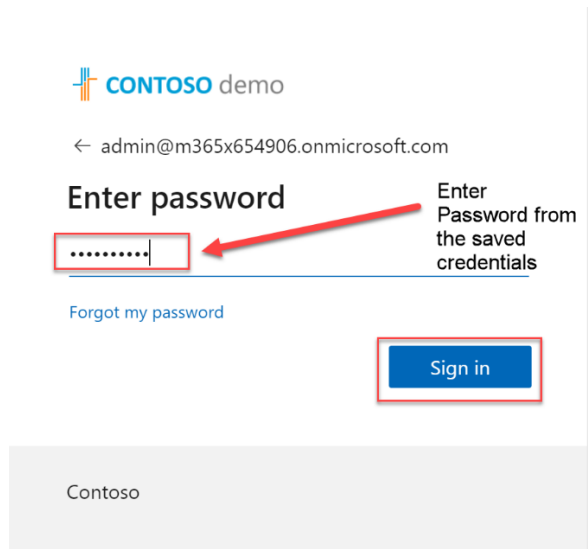
Open an In-private browser (Edge)  or New in-Cognito (Chrome)  on your machine and then go to <https://compliance.microsoft.com/homepage>

Enter the admin account username that you saved in "Getting started with Microsoft 365 Compliance Master Class Labs" to gain credentials.

- a) Enter your admin credentials in the sign in as below and click NEXT



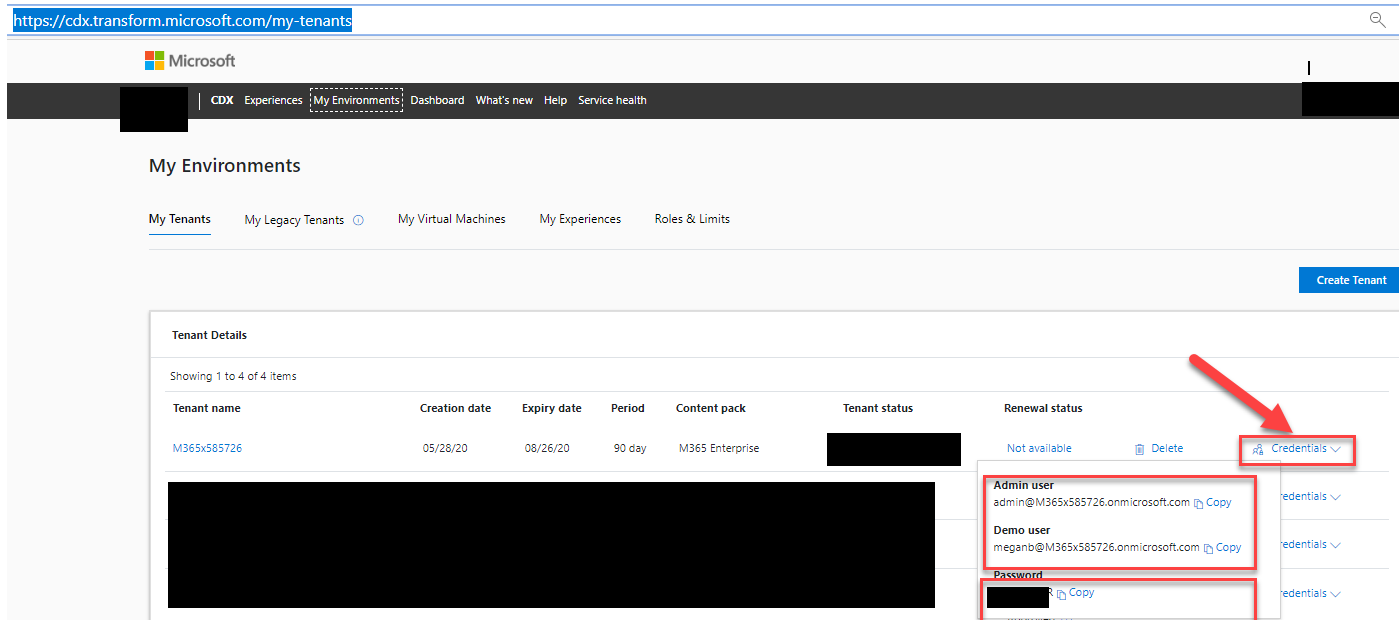
- b) Enter the password and then click "Sign in"



The recommended demo personas to use for performing demos in this guide, unless otherwise stated, are:

- Administrator scenarios: admin@<tenant>.onmicrosoft.com
- NestorW@<tenant>.onmicrosoft.com

The default password for both users can be found on your tenant information card at <https://cdx.transform.microsoft.com/my-tenants> (see picture below)



Lab Setup

Not all features used in this presentation are provisioned in your demo tenant!

This section will walk you through creating the Advanced eDiscovery Case, Investigation – 190301, and the Searches that you will use in the lab.

NOTE: Data analysis, content indexing, and preparing the results for analysis take time to complete so you may not be able to complete this in one sitting

1. Browse to <https://aka.ms/m365masterclass-labs> and download the **advanced_eDiscovery.zip** file. This file contains the supporting content needed to present the **Load non-Office 365 data** portion of the lab.
 - a. Download the file to your local computer and extract the files to the **%USERPROFILE%\Downloads\nonO365** on your computer.

Tip: You can also go to "downloads" folder, and create a new folder "nonO365" then move the files to this folder
 - b. Navigate to the **%USERPROFILE%\Downloads\nonO365** directory.

- c. Update the directory names to reflect the tenant you are using to demo: (see picture below as to where you find your tenant name)
- ChristieC@M365xTENANT.OnMicrosoft.com
 - NestorW@M365xTENANT.OnMicrosoft.com

The screenshot shows the Microsoft CDX 'My Environments' page. The navigation bar includes 'CDX', 'Experiences', 'My Environments', 'Dashboard', 'What's new', 'Help', and 'Service health'. The main content area is titled 'My Environments' and has tabs for 'My Tenants', 'My Legacy Tenants', 'My Virtual Machines', 'My Experiences', and 'Roles & Limits'. A 'Create Tenant' button is in the top right. Below is a table of tenants:

Tenant name	Creation date	Expiry date	Period	Content pack	Tenant status	Renewal status	
M365x585726	05/28/20	08/26/20	90 day	M365 Enterprise	[REDACTED]	Not available	Delete Credentials

2. Download and install Microsoft Azure Storage AzCopy.

- Open a new **Microsoft Edge** browser session and navigate to <https://docs.microsoft.com/en-us/azure/storage/common/storage-use-azcopy>.
- Click the link to download the latest version of AzCopy on Windows.
- Save the installer file for AzCopy on your local system.
- When the file has finished downloading, click **Run**, and then complete the setup wizard to install Microsoft Azure Storage AzCopy.

IMPORTANT: Note the path to azcopy.exe for later use.

Note if you are having issues go to : <https://docs.microsoft.com/en-us/previous-versions/azure/storage/storage-use-azcopy#download-and-install-azcopy-v81-on-windows>

3. Assign Mod Administrator as an eDiscovery Manager.

- a. Open **Microsoft Edge** and start a new InPrivate browser session.
 - b. Navigate to <https://protection.office.com/permissions>.
 - c. Log in with your global admin credentials: admin@<tenant>.onmicrosoft.com, and tenant password.
 - d. In the Microsoft 365 Compliance center, in the left navigation, click **Permissions**.
 - e. On the **Permissions** page, click **eDiscovery Manager**.
 - f. On **eDiscovery Manager** fly-out, scroll down to **eDiscovery Manager** click **Edit**.
 - g. On the **Editing Choose eDiscovery Manager** Page, click **Choose eDiscovery Manager**.
 - h. Click **+ Add**, and then type **MOD**.
 - i. Select **Mod Administrator** click **Add**, and then click **Done**.
 - j. Click **Save**, and verify **Mod Administrator** is displayed as an **eDiscovery Manager**.
 - k. On the **eDiscovery Manager** page, click **Close**.
 - l. Log out and close all browser windows. Note this is a critical step and may take some time to be resolve in system.
4. Set up the Advanced eDiscovery Case.
- a. Open **Microsoft Edge** and start a new browsing session.
 - b. Navigate to <https://compliance.microsoft.com>.
 - c. Log in with your global admin credentials: admin@<tenant>.onmicrosoft.com, and tenant password.
 - d. In the left navigation, click **eDiscovery**, and then click **Advanced eDiscovery**.
 - e. Select **Cases** from the top Menu
 - f. In **Cases**, click the **Create a case** to create a new case.
 - g. On the New eDiscovery Case page create a new case as follows:
 - Case name: **Investigation - 190301**
 - Case number: **190301**
 - Do you want to configure additional settings after creating this case?: **No, just go to the home page. I'll use the default case settings for now**
 - h. Click **Save**.
5. Add custodians to the Advanced eDiscovery case:

a. On the **Investigation - 190301** page, click the **Custodians** tab.

Note: If you don't see the **Custodians** tab, log out of the Microsoft 365 Compliance Center and close all browser windows. Open a new browser window and navigate to Microsoft 365 Compliance Center > eDiscovery > Advanced eDiscovery.

b. Click **+ Add custodians** and in **Choose Custodians** section add the following users to the case:

- Nestor Wilke
- Isaiah Langer
- Christie Cline

c. Click **Next**.

d. On the **Choose custodial locations** page, verify **Exchange** and **OneDrive** are selected as data sources, and then click **Next**.

e. On the **Select additional locations** page, on **Nestor Wilke**, click **Add**.

f. On the **Select additional locations for Nestor Wilke** page, click **Choose teams**.

g. On the **Edit locations** page, click **Choose teams**, click **Mark 8 Project Team**, and then click **Choose**.

h. On the **Edit locations** page, click **Done**, and then click **Save**.

i. On the **Select additional locations** page, click **Next**.

j. On the **Place a hold on the selected custodians** page, verify **Hold** is selected for the custodians, and then click **Complete**.

Note: On the **Investigation** page, ensure the **Indexing Job Status** for the custodians is **Successful**, before you continue.

6. Set up Searches

a. On the **Investigation - 190301** page, click the **Searches** tab, and then click **New search**.

b. On the **Name and description** page, in the **Name** field, type **Search for custodial data from relevant dates** and click **Next**.

c. On the **Custodians** page, enter the names of the suggested custodians (i.e. Nestor Wilke, Isaiah Langer, Christie Cline), and then click **Next**.

d. On the **Locations** page, click **Next**.

e. On the Search criteria page, click **+Add conditions**.

f. Select **Date**, then click **Add**.

- g. Configure the date as follows:
 - Date > Between: **2001-01-01** and **<current date>**
 - h. Click **Next**.
 - i. On the **Review your search** page, review your selections, click **Run**.
7. Create a review set.
 - a. On the **Investigation - 190301** page, click the **Review Sets** tab.
 - b. Click **+ Add Review Set**.
 - c. On the **Add Review Set** page, under **Review Set Name**, enter **Custodial Data**, and click **Save**.
8. Configure audit activity logging for Nestor Wilke.
 - a. On the **Investigation - 190301** page, click the **Custodians** tab, then select **Nestor Wilke**.
 - b. On the **Nestor Wilke** details page, click **View custodian activity**.
 - c. If necessary, click **Start recording user and admin activities**, then click **Turn on**.
 - d. Log out as the Mod Administrator and close all browser windows.
9. Seed audit activity logging for Nestor Wilke.
 - a. Open **Microsoft Edge** and start a new browser session.
 - b. Navigate to <https://office.com>.
 - c. Log in as NestorW@<tenant>.onmicrosoft.com. (To get Nestor's password if you have not used it before [click here](#))
 - d. Click **"X"** to close the first run experience.
 - e. Click **OneDrive** and open/close three or four files.
 - f. Log out as **Nestor Wilke** and close all browser windows.
10. Create Attorney Client Privilege CSV file
 - a. Open **Microsoft Excel** and create a new file
 - b. Enter the email alias **for GradyA (GradyA@<tenant>.onmicrosoft.com)** and **JoniS (JoniS@<tenant>.onmicrosoft.com)** on separate lines
 - c. Save file in CSV format and named "ACP.csv"

Part 2 - Advanced eDiscovery

As more customers adopt digital transformation, they also need an eDiscovery solution that allows them to quickly respond to regulatory and compliance requests efficiently. Whether it is litigation, internal investigation, responding to a regulatory request or policy obligation – you need to be able to find relevant content, refine that content and prepare that content to be handed off to the requesting body in an efficient and effective way.

Microsoft 365 Compliance Center: Case Creation

Lab Script	Click Steps
<p>The need for organizational search, also referred to as eDiscovery is becoming more and more prevalent. We estimate that less than 10% of all investigations are in response to legal action. You may for example, need to investigate an employee leaking or stealing sensitive information that potentially violates the code of conduct in your organization.</p> <p>Equally we are seeing a growing number of privacy related regulations of specific legal compliance such as GDPR that give individuals the right to request the information held on them. This can be a monumental task if you don't have a solution in place.</p> <p>Advanced eDiscovery for Microsoft 365 provides an effective way to manage information requests whether it is litigation, internal investigations, responding to a regulatory request or policy obligation. With Advanced eDiscovery you can create a case, add case members, put custodians on hold, send hold notifications, cull and review content and finally export only the most relevant content when needed.</p> <p>Let's walk through the steps of creating and managing a case using the Microsoft 365 Security and Compliance Center.</p>	<p>Create a new Case</p> <ol style="list-style-type: none">1. On the Advanced eDiscovery page, click Create a case located above the list of cases.2. On the New eDiscovery Case page create a new eDiscovery case as follows:<ul style="list-style-type: none">• Case name: Investigation - 01234• Case number: 01234• Do you want to configure additional settings after creating this case?: No, just go to the home page. I'll use the default case settings for now3. Click Save.

Lab Script	Click Steps
<p>The first step is creating a new case.</p>	
<p>Once you have created the case, you can configure case settings depending on the type of case it is, and the complexity expected.</p> <p>The Settings tab is used to configure search analytics within the case level.</p>	<p>Settings – Analytics settings and / or basic information</p> <ol style="list-style-type: none"> 1. On the Investigation - 01234 page, click the Settings tab. 2. In the Search & analytics section, click Select. 3. Review the settings for Analytics. 4. Select the checkboxes and change the following settings: <ul style="list-style-type: none"> • Document and email similarity threshold: 70% • Max number of themes: 10 5. Click Save, then click ← Back

Custodian Management & Communications

Lab Script	Click Steps
<p>Using custodian management and communications you can manage the eDiscovery workflow around identifying, collecting, and preserving potentially relevant information. First custodians are added to the case.</p> <p>A workflow will guide you through the process adding custodians to the case, configure the data sources associated with the person that are important to monitor and place a hold on the custodians.</p>	<p>Add Custodians to a Case</p> <ol style="list-style-type: none"> 1. On the Investigation - 01234 page, click the Custodians tab. 2. On the Choose custodians page, click + Add custodians and add the following users to the case: <ul style="list-style-type: none"> • Nestor Wilke • Isaiah Langer

Lab Script	Click Steps
<p>Let's review how this is done...</p> <p>Not only can you choose the custodial locations such as Nestor's email inbox and OneDrive for Business, but you can also quickly locate the shared locations Nestor has access to such as Teams, Yammer Groups, or Sites.</p> <p>In this case, you want to make sure that the Teams content from a Mark 8 Project Team is also on hold as part of this case.</p> <p>When Teams content is put on hold, you can feel confident that the Teams private channel messages and files are included in the hold.</p> <p>Similarly in the case of Yammer Groups, all posts, group documents, and messages are preserved when placed on hold.</p>	<ul style="list-style-type: none"> • Christie Cline <ol style="list-style-type: none"> 3. Click Next. 4. On the Choose custodial locations page, verify Exchange and OneDrive are selected as data sources, and then click Next. 5. On the Select additional locations page, on Nestor Wilke, click Add. 6. On the Would like to select additional sources for Nestor Wilke page, click Choose teams. 7. On the Edit locations page, click Choose teams, click Mark 8 Project Team, and then click Choose. 8. Optional: On the Edit locations page, click Choose yammer, click a group, and then click Choose. 9. On the Edit locations page, click Done, and then click Save. 10. On the Select additional locations page, click Next. 11. On the Place a hold on the selected custodians page, verify Hold is selected for the custodians, and then click Complete. 12. On the Investigation - 01234 page, click Back, to return to the Advanced eDiscovery page. <p>Note: to see Yammer, your Yammer network will need to be in Native Mode. If your network was provisioned after January 9th, 2020, you are already in Native Mode. If your network was provisioned <i>before</i> January 9th, 2020, you will need to follow the steps in the Overview of Native Mode.</p>

Lab Script	Click Steps
<p>Organizations are often required to inform custodians that they are on legal hold and need to be able to track when the custodians have been notified and when they acknowledged the legal hold. Organizations now can manage their legal workflow around custodian communications from within Advanced eDiscovery in the Compliance Center.</p> <p>Admins can send, collect, and track legal hold notifications. You can customize the hold notification workflows and content to meet your organization's needs.</p> <p>You can pre-fill notifications such as reminders and escalations. While creating these notifications, you can add links to ensure that custodians acknowledge receiving this information.</p> <p>A rich text editor is provided to create the Hold Notice and variables are available that can be used to create the notice.</p> <p>The admin can define if this is a new issuance, re-issue or release of hold for the communication and define the content within the hold as well as utilize common variables such as display name, acknowledgement link and more.</p>	<p>Create and send hold notification</p> <ol style="list-style-type: none"> 1. Click the Communications tab for case 01234 and select + New Communication. 2. Create a new policy as follows: <ul style="list-style-type: none"> • Name: Hold Notification • Issuing officer: Mod Administrator 3. Click Next. <p>Note: All custodial notifications will be sent on behalf of the Issuing Officer.</p> <ol style="list-style-type: none"> 4. Create the Hold Notice by using the rich-text editor and merge fields. You can copy the letter from Portal Content. In the text editor, highlight Replace with ACKNOWLEDGEMENT LINK, then click the Acknowledgement Link button located at the top of the editor to insert the merge field. 5. Once the portal content is created, click Next. 6. On the Set Notifications – Required page, click Edit and create new Issuance, Reissue, and Release notifications as follows: <ul style="list-style-type: none"> Click Save after creating each notice. These emails will include the Hold Notice appended to the end of the message. <p>Issuance:</p> <p>Subject: Issuance of Hold Notification</p>

Lab Script	Click Steps
	<p>Body: TO: {{DisplayName}} This is the issuance of the hold notification. The hold notification is attached. {{IssuingOfficerEmail}}</p> <p>Reissue:</p> <p>Subject: Reissue of Hold Notification Body: TO: {{DisplayName}} This is the reissue of the hold notification. The hold notification is attached. {{IssuingOfficerEmail}}</p> <p>Release:</p> <p>Subject: Release of Hold Notification Body: TO: {{DisplayName}} This is the release of the hold notification. The hold notification is attached. {{IssuingOfficerEmail}}</p> <ol style="list-style-type: none">1. After the required set notifications are created, click Next.2. On the Set Notifications – Optional page, click Next. The optional notifications include a Reminder and Escalation workflow to send recurring messages to the specified custodians and/or their manager.3. On the Choose the custodians you want to notify page, verify all custodians are selected and click Next.

Lab Script	Click Steps
	<ol style="list-style-type: none"> 4. On the Review your settings page, verify the settings and click Send. 5. Under Investigation – 01234, click Back to return to the Advanced eDiscovery page.
<p>Using the Custodians tab, users can view a custodian’s activity. This can be used to search and identify a custodian’s activity over time. Let’s review a case created in advance.</p> <p>This custodial activity view helps you understand a bit more about the people related to my case.</p>	<p><i>View custodian audit activity</i></p> <ol style="list-style-type: none"> 1. On the Advanced eDiscovery page, click Investigation – 190301. 2. On the Investigation - 190301 page, click the Custodians tab, then select Nestor Wilke. 3. On the Nestor Wilke details page, Click View custodian activity. 4. If necessary, click Start recording user activities, then click Turn on 5. Specify a date range and select Search to view recent custodian activity data. <p>Note: If no data is available, log in as Nestor Wilke and open a few files</p> <ol style="list-style-type: none"> 6. Click Close to close the Custodian activities page. 7. Click Close to close the details page for Nestor Wilke.

Searches

Lab Script	Click Steps
<p>After creating the case, adding the custodians and their associated data sources, the next step is to search for relevant content in the live Microsoft 365 tenant to build out the case.</p> <p>You can quickly do this by creating a new search.</p> <p>First you will name the search you want to build.</p> <p>Next, you will define the search criteria by adding conditions. Conditions are granular parameters such as dates, authors or even email recipients.</p> <p>You can also scope the search to the custodian content, and/or additional shared data locations if necessary.</p>	<p>Create a search</p> <ol style="list-style-type: none">1. On the Investigation - 190301 page, click the Searches tab, then click New search.2. On the Name and description page, in the Name field, type Search for Custodian Data and click Next.3. On the Custodians page, enter the name of each custodian to the search field.4. Click Next.5. On the Locations page, click Next.6. On the Search criteria page, click +Add conditions.7. Add a new condition as follows:<ul style="list-style-type: none">• Size (in bytes): Greater than > 08. Click Next.9. On the Review your search page, review your selections, click Run.
<p>After executing a search, you can use Statistics and Preview options to verify the search you created is collecting the type of data you need.</p> <p>Statistics provides a quick view of location of the results of your search and how many documents were found in those locations.</p>	<p>Preview results and search stats</p> <ol style="list-style-type: none">1. On the Investigation - 190301 page, on the Searches tab, select the search query: Search for custodial data from relevant dates and then click Statistics.

Lab Script	Click Steps
<p>Preview generates a sampling of the various data sources and provides a quick view for early validation that you are on the right track.</p> <p>You can also generate your own sample from a search using parameters such as confidence level and confidence interval.</p> <p>After you are satisfied with the statistics of the search, you can evaluate the content further by moving it into a review set.</p>	<ol style="list-style-type: none"> 2. On the Search Statistics page, on the Type drop-down list, select Summary and review the information. Repeat for the Top Locations and Queries types, and then click Back. 3. To review a sampled set of results, click More then click Sample, accept the defaults and click Next. 4. On the Add results to review set page, verify Custodial Data is selected, and click Send, then click Close.
<p>A review set is a static copy of documents that will help improve performance and stability of working with your content after you have validated the initial search results.</p> <p>With the review set, organizations can take an early pass at culling non-relevant content using various review features such as queries, filters, viewers that support office and non-office file types, a customizable coding panel and analytics.</p> <p>Adding the results of your search to a review set triggers the collection process.</p> <ol style="list-style-type: none"> 2. Advanced eDiscovery is going to collect all the content from your search results, 3. It will process all that content by extracting the text and metadata, 	<p>Done in step above</p>

Lab Script	Click Steps
<p>4. The results will be placed in a centralized index.</p> <p>5. These results from various sources can then be searched and analyzed through one interface</p> <p>If you want to add data from a source other than Office 365 into your search, a process is provided to add that data after you complete your initial search.</p>	
<p>If you have a very large volume of data, the Advanced eDiscovery dashboard enables you to view reporting and eDiscovery data visually.</p> <p>Even before you start your review process, the dashboard can help you quickly analyze your content in the review set to identify trends or key statistics and develop your review strategy. The dynamic dashboard is customizable so you can add, remove and configure widgets appropriate to your case and drill down into your content through the visuals.</p> <p>Here for example I only want to review all the cases from a specific sender domain. To do this, I will create a widget that allows me to see that data with a bar chart. Once I create the widget, I can then use this to help me craft my search. By applying a condition to the widget I can further filter down my search, which in this example I only want to see by senders domain. Once I specify the domain I can use this to create my search and save it as a query.</p>	<p><i>Use dashboard to develop review strategy</i></p> <ol style="list-style-type: none"> 1. Select Review Sets and open Custodial Data review set 2. On Individual results click Search profile view 3. Click +New widget then Create custom widget 4. Add Title and Choose pivot (sender domain) and Choose chart type (bar) then click Next 5. Click on widget then on the top right corner of the widget click Apply condition 6. Click on desired senders domain in chart 7. Add to search query add name under Please specify query name then click save 8. Click back to Review set 9. Click on Filters and review saved search query

Review set Management

Lab Script	Click Steps
<p>As part of the review set, you can configure a customizable tagging panel to organize your content. For example, you can create tags that identify content as responsive or non-responsive, privileged, etc. Later you can use these tags for workflows downstream such as redacting sensitive content on only the data tagged as “responsive”, or export all content tagged “ready for export”.</p> <p>This helps reviewers with early classification and culling of data to limit exports to the most responsive and relevant set of data.</p> <p>You can also leverage pre-trained Machine Learning models to help you identify potentially sensitive content. To use the models, you simply need to add smart tags sections to your tag panel.</p>	<p>Configure tag panel</p> <ol style="list-style-type: none">1. On the Investigation - 190301 page, on the Review Sets tab, click the Custodial Data review set,2. On the Custodial Data page, click Manage Review Set.3. Under Tags, click Manage tags. <p>NOTE: See Fig.1 at the end of this document for a screenshot of what the final tag panel should look like, and sequence of creation detailed below.</p> <ol style="list-style-type: none">4. On the Custodial Data, Tags page, click +Add section.5. Add a section as follows:<ul style="list-style-type: none">• Enter section title: Responsiveness• (Optional) Enter description: Responsiveness selections6. Click Save.7. On the Responsiveness section, click the vertical ellipsis, and click + Add option button.8. Below the Responsiveness section, on the new Selection item, click the Enter selection label field and type Responsive.9. Click Save.10. On the Responsiveness section, click the vertical ellipsis, and click + Add option button.

Lab Script	Click Steps
	<p>11. Below the Responsive selection, on the new Selection item, click the Enter selection label field and type Non-responsive.</p> <p>12. Click Save.</p> <p>13. On the Responsiveness section, click the vertical ellipsis, and click + Add option button.</p> <p>14. Below the Non-responsive section, on the new Selection item, click the Enter selection label field and type Needs further review.</p> <p>15. Click Save.</p> <p><i>Adding smart tag sections to a tag panel</i></p> <p>NOTE - To use these models, you will first need to opt in via the main Advanced eDiscovery home page. Steps below need to be done once for this tenant:</p> <p>To enable smart tags, start by enabling the feature</p> <ol style="list-style-type: none">1. On the Advanced eDiscovery page, click cases then click configure global analytics settings.2. Click the Manage attorney-client privilege setting button.3. Toggle the Attorney-client privilege detection to On.4. Click the Choose File button and browse to [steps to select Acp.csv], then click Save.5. Click Close. <p>Once smart tags are enabled:</p>

Lab Script	Click Steps
	<ol style="list-style-type: none"> 1. On the Investigation - 190301 page, on the Review Sets tab, click the Custodial Data review set, 2. On the Custodial Data page, click Manage Review Set. 3. Under Tags, click Manage tags 4. On the Custodial Data, Tags page, click the down arrow on the + Add section button, then click Add smart tag group. 5. Select the Attorney Client Privilege [BETA] model. 6. When finished adding sections, click Manage review set. 7. On the Custodial Data / Manage review set page, click View files. 8. When finished, click ←Review sets. <p>NOTE – This will add a new section along with tags to identify privileged and non-privileged content. You can rename these tags if preferred.</p>
<p>A Review set can include multiple collections of data. These collections are called Load Sets. Each Load Sets represent an individual collection loaded into the review set, whether loaded from Office 365, Non-Office 365 data or another review set.</p> <p>When data is loaded from Office 365, you can compare Load Sets from similar searches to understand what data was added from each load set.</p> <p>Select compare load sets to gain further insights into differences in load sets within a review set.</p>	<p><i>Understand differences between search results with load sets</i></p> <ol style="list-style-type: none"> 1. On the Investigation – 190301, click Custodial data, then click Manage Review set. 2. Under Load sets, click Manage load sets. <p>OPTIONAL: In the Load sets page, you can see all types of data loaded into the review set, Office365, Non-Office365 and other review sets. You can select two load sets to see</p>

Lab Script	Click Steps
	<p>the delta by selecting Compare load sets button. This will take several minutes to execute.</p> <p>3. When finished reviewing load sets, click ← Manage review set.</p>
<p>In many cases, organizations will need to include data from sources other than Office 365. In order to do that, Advanced eDiscovery provides a process for uploading that content.</p> <p>You can quickly create a container for non-Office 365 data and upload data into that container for inclusion in the case.</p>	<p>Load non-Office 365 data</p> <ol style="list-style-type: none"> 1. On the Custodial Data / Manage Review set page, in the Non-Office 365 data box, click View uploads. 2. On the Non-Office 365 data page, click Upload files. 3. Before you click Next: Upload files, carefully read the Prepare instructions and organize the files as instructed. 4. On the Upload files page, verify the path to the non-Office 365 files and the path to azcopy.exe, and click Copy to clipboard. 5. Click the start menu, type command, right-click Command Prompt, then click Run as administrator. 6. Right-click the title of the Command Prompt, select Edit and then click Paste. <p>NOTE: The command line will resemble something like this:</p> <pre>"%ProgramFiles(x86)%\Microsoft SDKs\Azure\AzCopy\AzCopy.exe" /Source:"C:\Users\name\Documents\eDiscovery\nestorw@M365x827261.onmicrosoft.com" /Dest:"https://spnam03salinkexternal001.blob.core.windows.net/89a0a114-361e-4aae-8335-351d14a7984b-1571322056-externalstore?sv=2017-07-29&sr=c&si=ExternalStore63%7C0&sig=LAAHzOVp91%2BA9fXWVWS4mA1N4jzykd086pMp49aOnLU%3D" /s</pre>

Lab Script	Click Steps
	<p>7. After the command is pasted, hit <Enter> in the command prompt. Verify the files have uploaded.</p> <p>8. Return to the Non-office data wizard and click Next: Process files.</p> <p>Note: Depending on the size and number of files, it will take time for the files to be processed. The Process stage will let the user monitor the progress of this Job. Once the files are uploaded, they will be available in the review set.</p> <p>9. You do not have to wait for the files to finish processing to click Non-office data.</p> <p>10. On the Non-Office 365 data page, click Refresh to view status of the files being processed, and then click Manage review set.</p>

Review and Tagging

Lab Script	Click Steps
<p>Now that documents are collected, you can analyze, review, and organize the content. You will run analysis first to minimize the number of documents you need to review, and query within a review set to find the set of documents you want to review. If the documents contain sensitive information, you may want to redact those parts. You can tag documents for further action.</p> <p>An integrated review experience offers the ability to view a wide variety of file types, including jpgs, all office files, mp4s and more, and to take action on that content. Either tag and further refine content based on its responsiveness, or annotate, mark-</p>	<p>Run eDiscovery analytics</p> <p>11. On the Review Set page and after clicking on Custodial Data, click on Manage review set, in the Analytics box, click Run analytics for the whole .</p> <p>12. In the Compliance dialog, click Yes, then OK.</p> <p>13. OPTIONAL: To view the status of the analytics job:</p> <ol style="list-style-type: none"> On the Custodial Data / Manage review set page, click View report, and then click Review sets.

Lab Script	Click Steps
<p>up and redact content that might be sensitive and should not be shared with outside parties.</p>	<ul style="list-style-type: none"> b. Go back to the Investigation - 190301 page, then click the Jobs tab. c. On the Jobs tab, review the status of Running analytics. d. When the status is Successful, click the Review sets tab, and then click the Custodial Data review set. e. On the Custodial Data page, click Manage Review set. <p>14. Under Analytics, click View report and review the report.</p> <p>NOTE: Due to processing time, the report may be unavailable. If presented with "This review set is being analyzed; please check back when analysis is complete. Please click the refresh button to check its latest state" click Refresh.</p> <p>15. When finished reviewing the report, click Manage review set.</p> <p>16. On the Custodial Data / Manage review set page, click View files.</p>
<p>After a Review set is created, queries can be created to start consuming the analytics data. You can create a search that only displays unique documents and suppresses all duplicates and noise. If two users are going back and forth 50 times, all the emails aren't displayed, just a couple of emails, inclusive of the email thread, reducing all the noise.</p>	<p>Query within a review set</p> <ul style="list-style-type: none"> 1. On the Investigation – 190301 > Review sets page, at left in the Saved Queries panel, click New Query. 2. Under Name, in the New query field, type Inclusive and Pivots. 3. Click + Add a condition. 4. In the Add a condition pane, in the Search box, type Inclusive.

Lab Script	Click Steps
<p>Creating a query lets you start viewing the data in themes by letting the system sort the content into buckets for easier review.</p> <p>By iterating the searches, you can narrow your focus to the content of interest.</p>	<ol style="list-style-type: none"> 5. Click the Inclusive type check box, then click Add. 6. On the drop-down list, verify Equals any of is selected. 7. In the Inclusive type condition, click Inclusive. 8. Click Add a condition. 9. In the Add a condition pane, in the Search box, type Marked as Pivot. 10. Click the Marked as Pivot check box, then click Add. 11. Under Marked as Pivot, click the Yes check box. 12. Click Save. 13. OPTIONAL: Scroll the window down to review the list of filtered items.
<p>The review experience includes a native, text and annotate view to provide options to support the various ways your team assess content.</p> <p>You can view the content in a viewer in the document's native format. While viewing the document you can redact content allowing you to export the content with some of the information redacted.</p>	<p>Annotate a document</p> <ol style="list-style-type: none"> 1. In a Review set, select an email, and click to open. NOTE: Not all content will be viewable. If presented with "Sorry!, File not supported. You can download the file, and process it offline" select another item from the content list. 2. In the File metadata window, click Annotate View. 3. Click the Drawing drop-down menu, then click Area redaction. 4. Click, then drag the mouse over a few of sentences to make a selection area. NOTE: The redaction will automatically fill the selected area.

Lab Script	Click Steps
	<p>5. To the right of the Drawing drop-down menu, click the Toggle Annotation Transparency icon, to view the redacted content.</p>
	<p><i>Bulk tagging</i></p> <ol style="list-style-type: none">1. On the Custodial Data review set page, select multiple documents by clicking the radio button to the left of each item.2. In the Tagging panel, under Responsiveness, click Responsive, and then under Legal advice, click Has legal advice.3. On the Custodial Data page click Review sets. <p>Note: In order to see "Legal advice" you must configure global analytics settings and under manage attorney-client privilege setting turn it to on.</p>

Jobs

Lab Script	Click Steps
<p>Any process in Advanced eDiscovery that takes more than a few seconds is created as a job. The Jobs tab tracks the status of jobs that are running or have been completed.</p>	<p>Overview of jobs</p> <ol style="list-style-type: none">1. On the Investigation – 190301 page, click the Jobs.2. Click the Filter button.3. Next to Type, click the down arrow to display the applied filters.4. Next to Type, click the up arrow to hide the applied filters. OPTIONAL: Repeat showing and hiding the applied filters for the Status and Scope sections.5. At left, under Type, select an item to expose its details pane.6. POINT OUT: in the details pane point to Job type, Status, Progress, and Sub jobs.7. At top right, click the Close (X) icon.

Errors

Lab Script	Click Steps
<p>Sometimes, the Office 365 services are unable to fully index a file. A common example of this is when a file is password protected. Error remediation allows you to fix errors and add the corrected files back into the system so the files can be processed as if the problem never occurred. In some cases, it's</p>	<p>Error reporting</p> <ol style="list-style-type: none">1. On the Investigation - 190301 page, click the Processing tab,2. Click the View drop-down, and then click Errors.

Lab Script	Click Steps
<p>not necessary to remediate errors but it's important to simply report the errors that were encountered.</p> <p>The errors tab lists all errors that were encountered and further breaks down the errors by file count and includes the number of items and the size.</p>	<ol style="list-style-type: none"> 3. Click the Scope drop-down, and then click Custodial Data. 4. Click to the left of File is protected to select it, then click + New error remediation. NOTE: Preparation may take a few minutes. 5. Review the remediation steps on the New remediation page, click Cancel, and then click Yes.

Export

Lab Script	Click Steps
<p>In some cases, a lawyer or another third party may just need to download five documents from a case for a specific deposition, and in that case, we provide the download option.</p>	<p><i>Download query results</i></p> <ol style="list-style-type: none"> 1. On the Investigation - 190301 page, click the Review sets tab, and then click on the Custodial Data review set. 2. In the Review set, select multiple documents by clicking the single select radio button to the left of the document. 3. Click the Action drop-down menu, then click Download. 4. In the UAC dialog, click Save.
<p>For bigger volumes, you can use the export option. You have several options for how to export the content, choose the one that makes the most sense in your context and export the relevant content to enable the next steps of your process.</p>	<p><i>Export query results to Microsoft provided Azure Blob</i></p> <ol style="list-style-type: none"> 1. In the Review set, on the Custodial Data page, click Saved queries. 2. On the Saved queries list, click Inclusive and Pivots. 3. Select multiple emails and/or documents by clicking the single select radio button to the left of the document.

Lab Script	Click Steps
	<p>4. Click Action and click Export.</p> <p>5. Complete Export Options as follows:</p> <ul style="list-style-type: none"> • Export Name: Custodial Data Export • Export Scope: Selected items • Export File location: Microsoft Provided Azure Blob Container <p>6. Click Export.</p> <p>7. In the A job has been created! dialog, click OK.</p>

Conclusion

Lab Script	Click Steps
<p>Lab CONCLUSION</p> <p>As you can see, Microsoft’s addition of Advanced eDiscovery to the Microsoft 365 Compliance Center enables companies to quickly find relevant emails and information across large quantities of stored email and document content. Even if stored in the cloud, Advanced eDiscovery streamlines discovery and analysis processes allowing organizations to respond to requests in a timely manner. Whether it is litigation, internal investigation, responding to a regulatory request or policy obligation – you’ll be able to find relevant content, refine that content, and prepare that content to be handed off to the requesting body in an efficient and effective way.</p>	<p>No Click steps</p>

Portal Content

You can copy the letter as follows and update the fields for the hold notice on the portal content:

Hold Order

Confidential

To: {{DisplayName}}

From: Office of General Counsel

Date: {{IssuingDate}}

The company has received a subpoena from SEC which will require the collection and production of certain company documents in connection with an investigation of insider trading. We intend to comply fully with the subpoena and to cooperate with the SEC investigation. A description of the documents covered by the subpoena is attached.

In order to fully comply with the SEC subpoena, it is vital that all documents described in the attachment (including hard copy documents as well as electronic data and documents) be preserved, and all routine destruction or discarding of any such documents or data, whether pursuant to formal company policies or otherwise, be suspended until further notice. This includes turning off any "autodelete" functions and insuring that back-up tapes are preserved and not overwritten or deleted. If you have a question about whether or not something needs to be preserved, err on the side of preserving it until advised otherwise by legal counsel.

This policy applies to all such documents whether kept at the office, at off-site storage facilities, or at your home. It includes not only formal company documents, but also materials such as handwritten notes, drafts, calendars and the like. In addition, if anyone under your supervision has custody or control of such documents or data and it is not listed as a recipient of this memorandum, please forward it to them immediately. If you know of others who should receive this memorandum, or if you know of documents beyond our control that should be preserved, please notify {{IssuingOfficerEmail}} immediately.

Detailed instructions regarding the procedures for collection of documents will follow shortly and will be designed to minimize disruption of your daily business activities. Until such instructions are provided, all documents and files should be maintained as they are kept in the ordinary course of business.

The subpoena should not be discussed outside of any discussions necessary for document preservation and compliance, or in communications with company counsel. There should be no discussions with third parties.

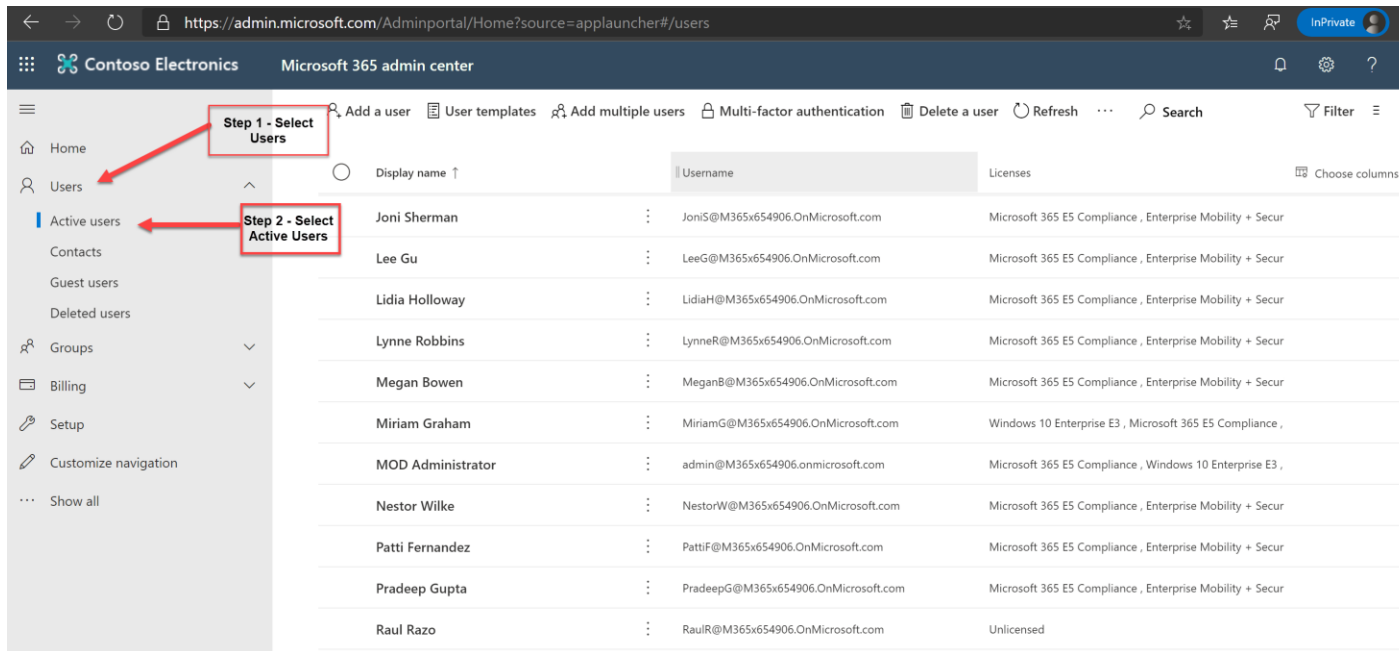
We require that you acknowledge this notice by clicking the link below.

Replace with ACKNOWLEDGEMENT LINK

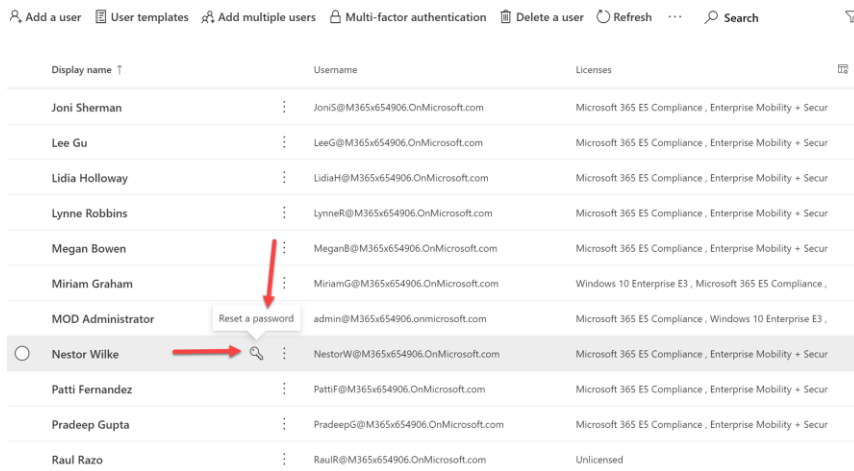
If you have any questions concerning this notice, please contact {{IssuingOfficerEmail}}

To get Nestor Wilke Credentials

- [NestorW@<tenant>.onmicrosoft.com](#) (You will need to reset this password yourself as its not in the default credentials)
- To complete password reset for NestorW – logon as MeganB@<tenant>.onmicrosoft.com to <https://admin.microsoft.com/Adminportal/>
 - On the right hand tab **select users > Active Users**



11. Hover over Nestor Wilke name and you will see a **Reset a password** – Select the key to reset the password.



12. Save the credentials so that you can logon as him in the later stages of this lab.

Reset password

NestorW@M365x654906.OnMicrosoft.com


Password settings

- Auto-generate password
- Let me create the password

Select this option

Enter a strong password

Password *

..... Strong 

Require this user to change their password when they first sign in

Untick this box

Click to reset password

Reset

13.